MULTIPLE LEVEL DATA HIDING MEDICAL IMAGE BASE ON *DISCRETE* COSINE TRANSFORM (DCT) METHOD USING MULTI-SCALE IMAGE SHARING (MSIS)

Tegar Palyus Fiqar[1)] dan Awang Pradana[2)]
[1, 2)] Jurusan Teknik Informatika, Fakultas Teknologi Informasi (FTIF),
Institut Teknologi Sepuluh Nopember, Surabaya, Indonesia, 60111
e-mail: tegar.pf@gmail.com[1)], dhanawinks@gmail.com[2)]

ABSTRAK

Pengiriman data melalui media elektronik semakin pesat. Banyak data yang gunakan transkasi internet adalah data rahasia. Salah satu data rahasia ialah data medis seorang pasien. Pada umumnya data medis pasien tidak hanya terdiri dari satu buah citra saja, melainkan data citra yang jumlahnya lebih dari satu. Sehingga diperlukan suatu mekanisme penyembunyian (steganografi) data medis pasien yang jumlahnya lebih dari satu kedalam sebuah media pembawa, agar data ini dapat terlindungi dari pihak-pihak yang tidak berkepingan. Pada penelitian ini menerapkan discrete cosine transform dalam steganografi citra. Cover dan pesan rahasia steganografi yang digunakan berupa citra dengan ukuran 512px X 512px. Pada proses penyisipan data rahasia yang jumlahnya banyak diterapkan denagn multi- level menggunakan sekma multi-scale image sharing (MSIS). Dalam proses pengujian digunakan citra cover 24 bit. Pada citra cover 24 bit yang digunakan memiliki format .png. Proses parameter analisis pengujian menggunakan Peak Signal to Noise Ratio, Mean Squared Error, Normalized Cross Correlation, Average Difference, Structural Content, Maximum Difference, Normalized Absolute Error serta dari sisi size. Hasil Peak Signal to Noise Ratio pada penyisipan level 1 dan level 9 bernilai kurang lebih 40 db dan 24 db.

***Kata Kunci**: Steganografi, Multiple level, DCT.*

ABSTRACT

Sending data through the electronic media is rapidly increasing.Many of the data used in internet transactions is confidential data. One of confidential data is a patient medical data. Generally the medical data of patients not only consist of a single image, but image data of more than one. So it requires a mechanism of concealment (steganography) patient medical data of more than one into a carrier, so this data can be protected from those who are not interested. In this study, applying the discrete cosine transform in image steganography. Cover and used steganography secret message in the form of the image with a size of 512px X 512px. In the insertion process confidential data polynomial is applied by using a multi-level scheme of multi-scale image sharing (MSIS). In the testing process used a 24-bit image cover. In the cover image of 24 bits used have a .png format. Process parameter test analysis using Peak Signal to Noise Ratio, Mean Squared Error, Normalized Cross Correlation, Average Difference, Structural Content, Maximum Difference, Normalized Absolute Error and from the size. Result of Peak Signal to Noise Ratio for level 1 and level 9 data hiding equal 40 db and 24 db.

Keywords: Steganography, multiple level, DCT.

I. PENDAHULUAN

PENGIRIMAN data melalui media elektronik semakin meningkat, seiring dengan kemudahan dalam melakukan akses internet dalam bentuk data. Tidak hanya individu yang melakukan akses internet melainkan pihak medis yang memiliki data bersifat rahasia juga dikirimkan melalui internet. Data yang dikirmkan dapat dalam berbagai bentuk format *file* baik dalam berbentuk teks, citra, audio maupun video. Tranksasi data internet semakin pesat sehingga diperlukan cara agar dapat menyembunyikan data rahasia dalam sebuah *file*. *Steganography* merupakan salah satu ckim]ara penyisipan data rahasia *hidden message* dalam sebuah *file cover* media pembawa. Citra medis merupakan citra yang memiliki sifat rahasisa, hal ini karena dalam citra medis terdapat informasi mengenai penyakit yang dialami oleh pasien. Pada umumnya citra medis yang digunakan untuk mendiagnosa suatu penyakit terdiri dari beberapa buah citra dari beberapa posisi pengambilan citra. Sehingga diperlukan suatu cara untuk menyembunyikan citra medis yang jumlahnya lebih dari satu dalam sebuah *file cover*.

Pada proses penyisipan pesan atau penerapan *steganography* dilakukan pada domain frekuensi untuk *cover image* dan beberapa *hidden image* dalam hal ini citra medis. Domain frekuensi yang digunakan yaitu *discrete cosine transform* (DCT)[1]. Sebelum citra diubah menjadi domain frekuensi, baik citra *cover* dan citra *hidden* diubah menjadi *grayscale*. *Grayscale* ini bertujuan merubah kedua citra *cover* dan citra *hidden* dari tiga kanal warna menjadi satu kanal warna.

Proses penyisipan citra *hidden* yang jumlahnya banyak diperlukan suatu mekanisme atau skema penyisipan. Skema yang digunakan *multi-scale image sharing*[2]. Skema ini dibangun berdasarkan *level* proses penyisipan

yang dilakukan. Pada proses Steganografi menggunakan *cover* dan *hidden message* berupa citra. Citra *cover* dan *hidden message* yang digunakan berukuran 512 x 512 *px*. Pengolahan Steganografi dalam domain frekuensi dengan menggunakan metode *Discrete Cosine Transform.*

II. STUDI LITERATUR

A. Multi-level data hiding

Salah satu penelitian yang terkait dengan *multi-level* yaitu teknik *encoding multi-level* menggunakan prinsip *psychoacoustical* dari *binaural*[3]. Teknik ini dikembangkan pada domain frekuensi 1 dimensi dan menggunakan sinyal *stereo audio*. Nilai ambang batas dari frekuensi dihitung dari selisih dari phase interaural. Selanjutnya digunakna untuk menentukan lokasi yang tepat untuk penyisipan data. Nilai ambang batas dibagi menjadi beberapa sub-*level*, masing-masing membawa beberapa *bit* data.

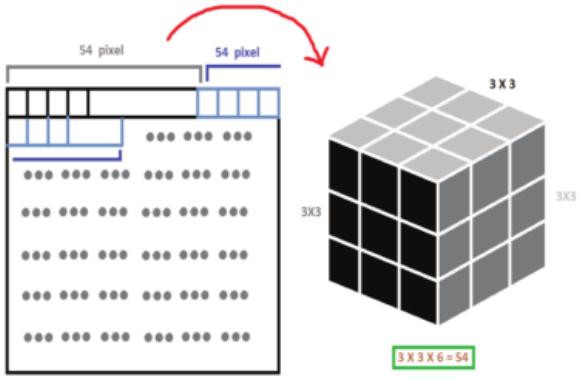
Penelitian selanjutnya mengenai *multi*- level data hiding yaitu dengan menerapkan mekanisme algoritma kubik rubik[4]. Alasan mengadopsi kubik rubik adalah karena memiliki 6 permukaan dan dapat dibagi menjadi 54 (6 permukaan * 3 * 3) elemen. Pada tahap awal, proses penyisipan gambar akan dibagi menjadi ukuran blok yang berbeda berdasarkan *pixel* tersebut, sebagai contoh berukuran 3 * 3 *pixel*, atau berukuran m * n *pixel*. Setelah itu, 54 unit blok akan dipilih secara berurutan dan diubah menjadi 6 permukaan sesuai dengan enam permukaan dari kubik rubik dengan diberikan nomor indeks. Selanjutnya gambar dibagi menjadi banyak 54 unit yang berbeda berdasarkan blok sehingga banyak membentuk kubik rubik yang berbeda. Setiap kubik rubik akan diberi nomor acak yang berbeda untuk melakukan rotasi. Mekanisme penyembuanyian data yang diusulkan dapat dilakukan dalam domain spasial, domain frekuensi, dan domain *hybrid*. Hal ini juga dapat dikombinasikan dengan encipher. Gambar 1 merupakan ilustrasi metode algoritma kubik rubrik.

Salah satu penyisipan pada domain spasial yaitu dengan melakkan subtitusi metode *least significant bit* (LSB) dan metode multi-*pixel differencing* (MPD)[5]. Metode ini dikembangkan bertujuan untuk meningkatkan kapasitas penyisipan dari data rahasia dan mingngkatkan kualitas secara visual. Tahap pertama melakukan perhitungan penjumlahan dari selisih nilai dari masing-masing 4 sub-blok *pixel*. Nilai penumlahan yang kecil diletakan pada smooth blok dan nilai yang besar diletakan pada edge blok. Data rahasia yang disembunyikan pada citra cover menggunakan metode LSB pada smooth blok dan metode MPD diletakna pada edge blok.

Penyembunyian data rahasia dengan menggunakan refrensi *pixel* dan penyisipan *multi*-layer dikembangkan dengan menfaatkan pergeseran selisih *pixel* pada histogram[6]. Selisih nilai *pixel* digenerate antara refrensi piksel dan tetangga piksel. Setelah pergeseran selisih histogram dilakukan maka tahap selanjutnya menyisipkan data rahasia pada *cover image*, dan *multi*-layer digunakan untuk meningkatkan kapasitas penyisipan. Perbedaan penelitan dengan sebelumnya yang berkaitan skema pergeseran histogram yaitu dapat mengekstrak data tersembunyi dan memulihkan gambar *cover* asli yang sebenarnya dengan tidak ada informasi tambahan kecuali panjang data yang tersembunyi dan stego-gambar itu sendiri.

Multi-level penyisipan data dapat dilakukan dengan mengguakan modifikasi *histogram* dari selisih citra[7]. Penelitian ini mengusulkan penyisipan data *multi-level* menggunakan mofikasi *histogram* dengan menggunakan titik puncak untuk menyembunyikan pesan rahasia. Metode ini dapat menyelesaikan permasalahan kapasitas dari data yang disembunyikan. Serta menjada distorsi yang rendah pada hasil steganografi.

Penyisipan data pada domain spasial dengan dua tahap *multi*-layer dengan skema interpolasi lagrange[8]. Interpolasi lagraange diterapkan pada prediksi ganjil dan genap piksel citra. Selanjutnya modifikasi pergeseran histogram digunakan untuk menyisipkan data rahasia kedalam selisih antara citra prediksi dan citra hasil.



Gambar 1. Algoritma kubik Rubrik

Sebuah skema semi-*fragile lossless* data hiding (LDH) dikembangkan dengan menggunakan distribusi persegeran histogram pada domain integer *wavelet transform* (IWT)[9]. Sekma ini dikembangkan dengan pendekatan trasformasi citra membagi menajadi blok yang tidak *overlapping*. Pada setipa blok, selisih antara *element* tetangga dihitung dan sebuah *histogram* dihasilkan nilai selisih. Data rahasia disisipkan kedalam blok dengan menggunakan mekanisme *multi-level* pergesaran dari *histogram*.

B. Aspek-aspek Steganografi

Penilaian sebuah algoritma steganografi yang baik dapat dinilai dari beberapa faktor yaitu:

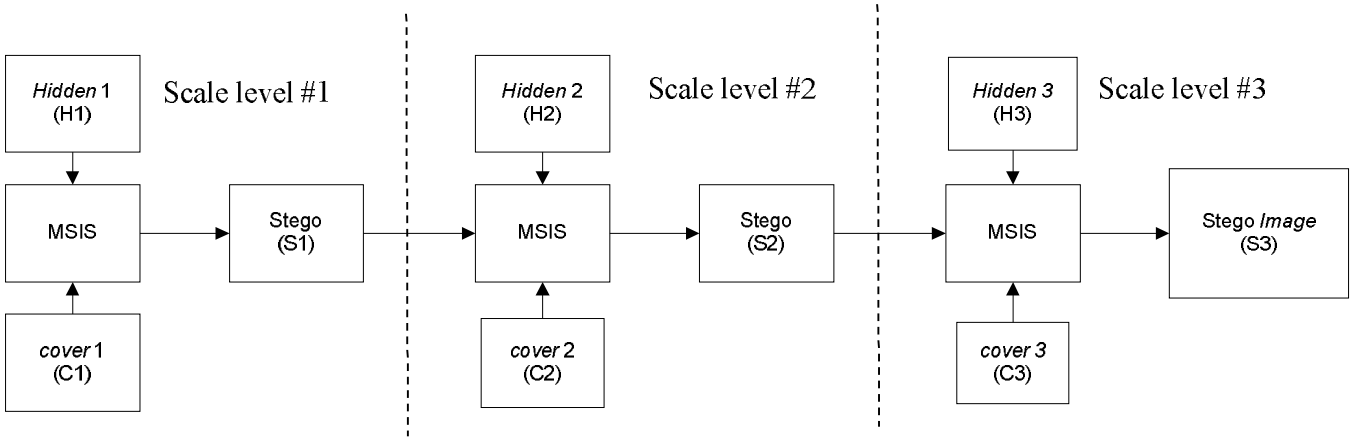
1. *Imperectibility*[1],[10],[11]
   Keberadaan pesan rahasia dalam media penampung tidak dapat dideteksi oleh inderawi. Misalnya jika *covertext* berupa citra, maka penyisipan pesan membuat citra *stegotex*t sukar dibedakan oleh mata dengan *covertext*-nya. Jika *covertext* berupa *audio*, maka indera telinga tidak dapat mendeteksi perubahan pada *stegotext*-nya.
2. *Fidelity*[1] ,[11]
   Mutu media penampung tidak akan berubah banyak akibat penyisipan. Perubahan ini tidak dapat dipersepsi oleh inderawi. Misalnya, jika *covertext* berupa citra, maka penyisipan pesan dapat membuat *stegotext* sukar dibedakan oleh mata dengan citra *covertext*-nya. Jika *covertext* berupa *audio*, maka audio *stegotext* tidak rusak dan indera telinga tidak dapat mendeteksi perubahan pada *file stegotext*-nya.
3. *Recovery*[1]
   Pesan yang disembunyikan harus dapat diungkapkan kembali. Karena tujuan steganografi adalah data yang tersembunyi, maka sewaktu-waktu pesan rahasia di dalam *stegotext* harus dapat diambil kembali untuk digunakan lebih lanjut.
4. *Size*[1],[10],[11]
   Ukuran dari *file* media pembawa dan media hasil sisipan tidak berbeda jauh.

III. METODE

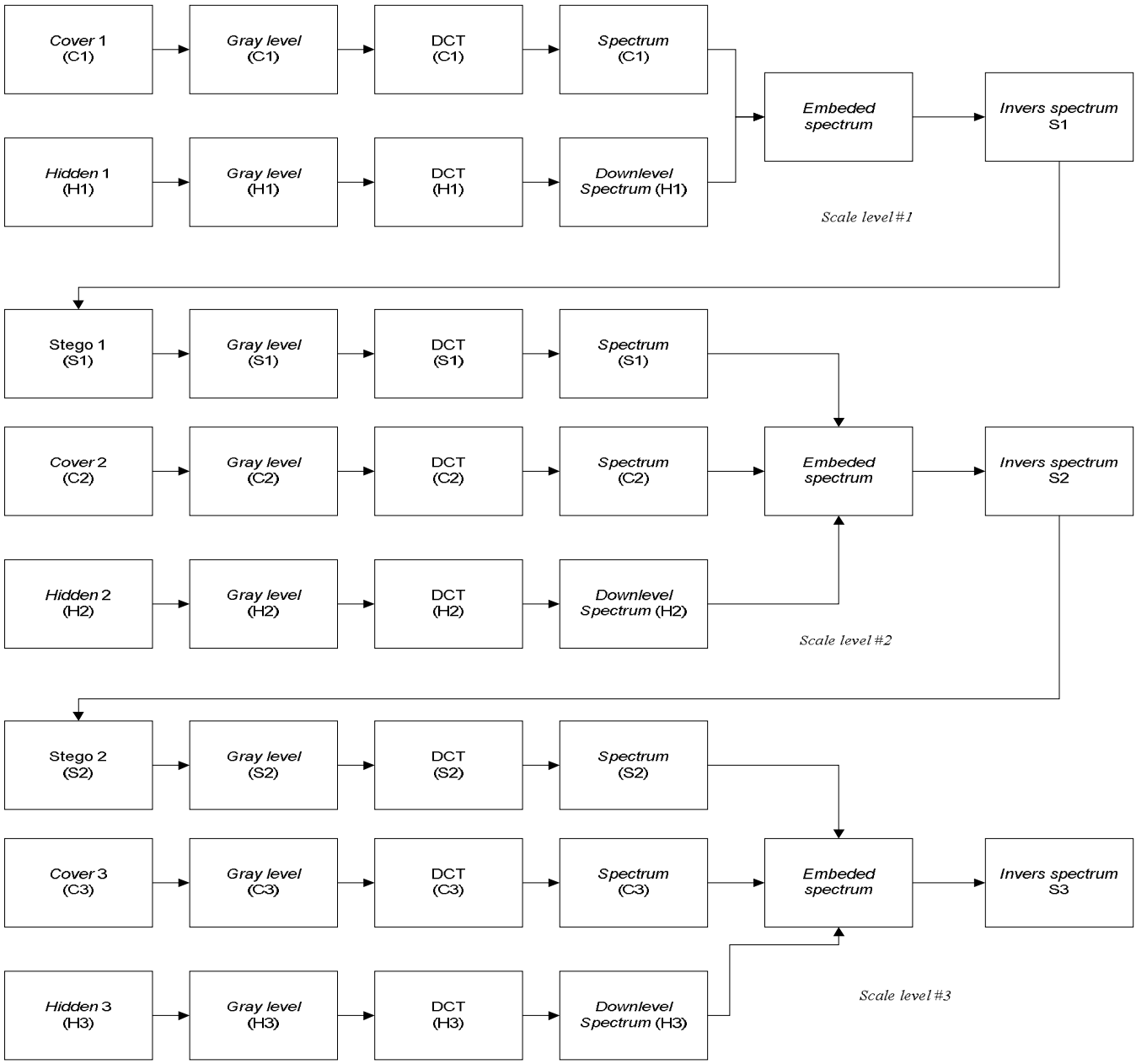
Pada penelitian ini kami melakukan modifikasi steganografi citra dengan *multi*ple *level* data. Penelitian ini menggunakan citra *cover* dan pesan rahasia berupa citra medis. Proses penyisipan pesan rahasia dilakukan dengan *discrete cosine* transfom.

Modifikasi steganografi dilakukan dengan melakukan penyisipan beberapa jumlah citra *hidden*. Proses penyisipan ini menggunakan skema *multi-scale image sharing* (MSIS)[2]. Skema metode MSIS yang digunakan dalam penelitian ini digambarkan pada gambar 2. Detail dari MSIS ini ditunjukan pada skema gambar 3.

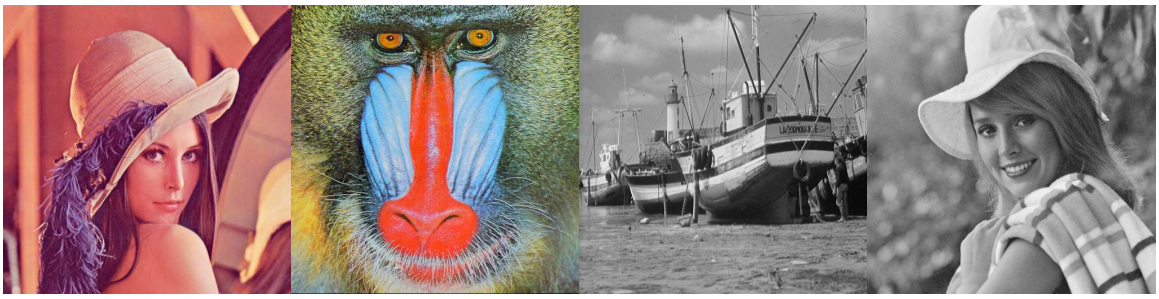
Dalam melakukan penelitian ini kami menggunakan bahasa pemrograman c++ dan Opencv sebagai *library* yang digunakan untuk melakukan pengolahan citra.



Gambar 2. Skema MSIS steganografi



Gambar 3. Skema Detail *MSIS* steganografi



(a) (b) (c) (d)

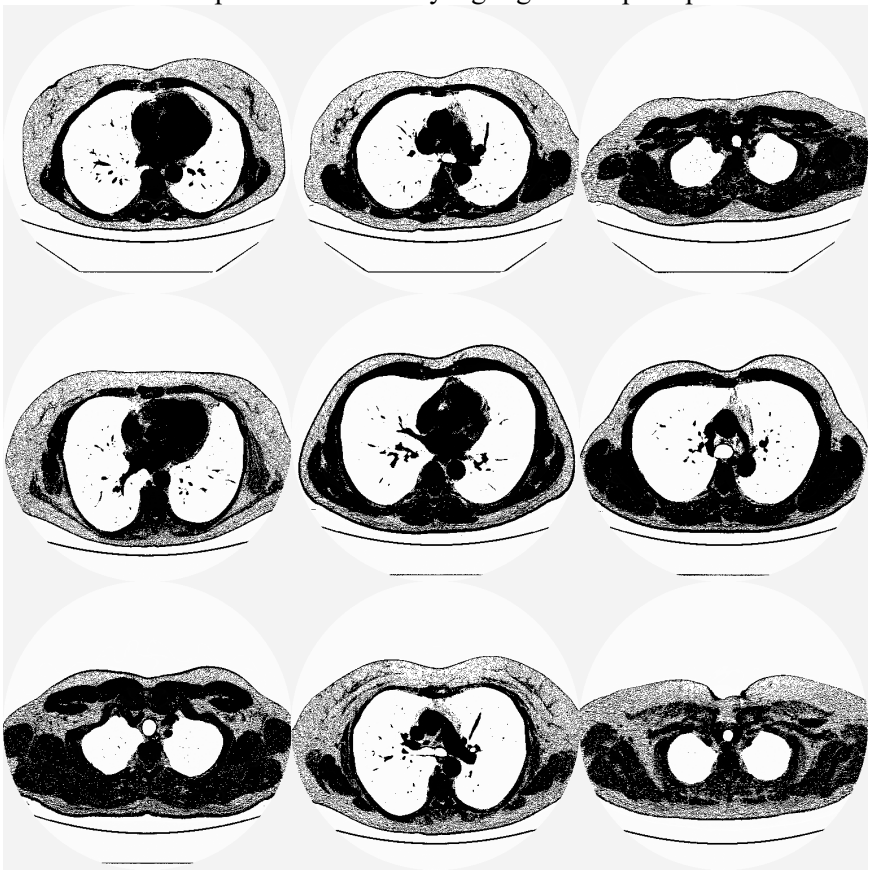
Gambar 4. Sampel citar *cover* (sumber: http://sipi.usc.edu/database/)

A. Cover citra

Pada penelitian ini menggunakan citra standar yang sering digunakan penelitian lainnya. Citra yang digunakan sebanyak 4 buah sampel. Ukuran yang digunakan yaitu 512px x 512px. Citra *cover* yang digunakan sebanyak satu jenis format. Format yang digunakan yaitu .png. 24 *bit color* diguanakan pada citra berformat .png. Citra *cover* yang digunakan seperti gambar 4.

B. Citra Rahasia

Citra medis yang digunakan merupakan potongan-potongan citra medis paru-paru. Citra rahasia yang digunakan berukuran 512 x 512 px. Pada database ini berisi 115 citra. Format *file* yang digunakan .tif dengan 16 *bit color*. Potongan-potongan citra ini gunakan dengan format [subjek]_[lokasi].tif. Pada penelitian ini digunakan 9 buah citra rahasia. Gambar 5 merupakan citra medis yang digunakan pada penelitian ini.

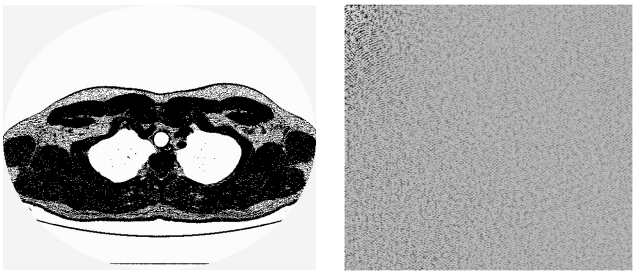


(a)	(b)	(c)
(d)	(e)	(f)
(g)	(h)	(i)

Gambar 5. Citar medis *rahasia (a) A0001_bottom, (b) A0001_middle, (c) A0001_top, (d) A0003_bottom, (e) A0003_middle, (f) A0003_top, (g) A0005_bottom, (h) A0005_middle, (i) A0005_top* (sumber: http://image.diku.dk/emphysema_database/)

(a)	(b)
(c)	(d)

Gambar 6. Proses *grayscale* (a) citra *cover* sebelum *grayscale*, (b) citra *cover* sesudah *grayscale,* (c) citra *hidden* sebelum *grayscale*, (d) citra *hidden* sesudah *grayscale*



(a) (b)

Gambar 7. (a) Citra *hidden* domain spasial, (b) Spektrum magnitude citra *hidden*

C. *Grayscale*

Sebelum citra ditransformasikan kedalam bentuk domain frekuensi maka citra tersebut harus diubah kedalam *grayscale*, hal ini bertujuan merubah kanal citra yang akan ditransformasikan, dari tiga kanal menjadi 1 kanal. Proses *grayscale* ini diterapkan baik pada citra *cover* dan citra *hidden*, berlaku juga pada semua citra *hidden*. Perubahan kanal ini bermaksud untuk mempermudah komputasi yang dilakukan. Proses *grayscale* seperti diilustrasikan gambar 6.

D. *Discrete Cosine Transform (DCT)*

Citra yang digunakan diubah menjadi domain frekuensi dari domain spasial, baik citra *cover* maupun citra rahasia. Citra yang berdomain spasial memiliki fungsi f(x,y) dari ukuran *pixel* M x N. Citra tersebut diolah menjadi domain frekuensi menjadi fungsi F(u,v). Transfomasi ini dikenal dengan transformasi *discrete cosine transform* dua dimensi[12]. Persamaan yang digunakan seperi pada persamaan (1).

$$F(u,v) = \frac{2}{\sqrt{M.N}} C(u)C(v) \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} f(x,y) \cos \frac{(2x+1)u\mu}{2M} \cos \frac{(2y+1)u\mu}{2N} \quad (1)$$

Dimana $u = 0,1,\ldots.M; v = 0,1,\ldots.N,$

$C(u) = \frac{1}{\sqrt{2}} untuk\ u = 0\ dan\ 1\ yang\ lainnya$

$C(v) = \frac{1}{\sqrt{2}} untuk\ u = 0\ dan\ 1\ yang\ lainnya$

E. *Spektrum Magnitude*

Hasil dari DCT direpesentasikan kedalam sebuah bidang frekuensi baru yang disebut spektrum magnitude. Hasil ini berada pada domain frekuensi. Proses ini diilustrasikan pada Gambar 7.

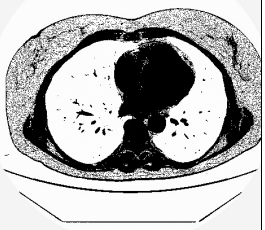
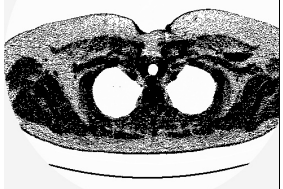
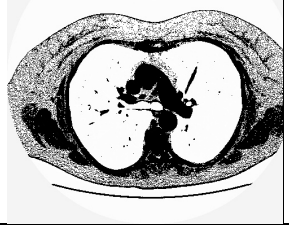
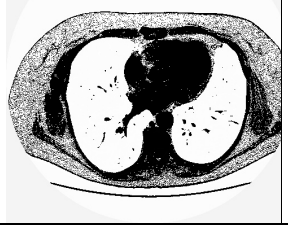
IV. HASIL PENGUJIAN

Dalam melakukan pengujian, kami melakukan dengan melakukan penyisipan sembilan buah data medis rahasia ke dalam sebuah citra cover lenna. Citra rahasia yang digunakan berupa citra medis. Citra medis yang digunakan bersumber dari *computed tomography emphysema database.* Data citra medis ini dapat diperoleh pada alamat http://image.diku.dk/emphysema_database/. Data ini didedikasikan untuk penelitian yang terkait sehingga tidak diperjualbelikan. Tabel 1 mengilustrasikan data rahasia pada domain spasial yang akan digunakan. Selanjutnya dari domain spasial data rahasia tersebut ditransformasi ke dalam bentuk frekuensi dengan menggunakan metode *discrete cosine transform*. Trannsformasi ini menghasilkan *spectrum* magnitude dari masing-masing data rahasia. Spektrum magnitude inilah yang digunakan dalam proses penyisipan.

Pada domain frekuensi penyisipan, level pertama dilakukan penyisipan antara *spectrum* magnitude *cover* dan data *hidden* pertama. *Level* kedua dilakukan penyisipan antara *spectrum* magnitude *cover*, *spectrum* data *hidden* 2 dan hasil *spectrum* pada *level* pertama. *Level* ketiga dilakukan penyisipan antara *spectrum* magnitude *cover*, *spectrum* data *hidden* 3 dan hasil *spectrum* pada *level* kedua. *Level* kempat dilakukan penyisipan antara *spectrum* magnitude *cover*, *spectrum* data *hidden* 4 dan hasil *spectrum* pada *level* ketiga. Proses penyisipan ini dilakukan hingga data *hidden* ke Sembilan. Pada Tabel 2 menunjukan proses *cover* dan data *hidden* pada masing-masing *level* penyisipan serta hasil setelah dilakukan penyisipan pada setiap levelnya.

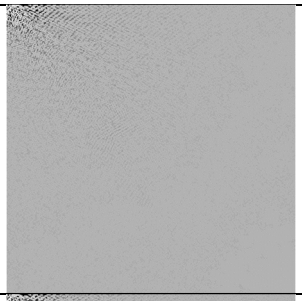
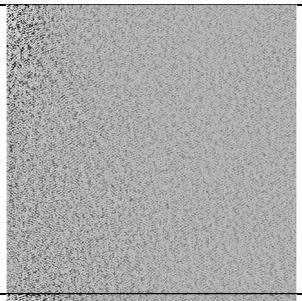
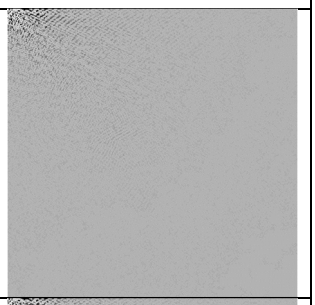
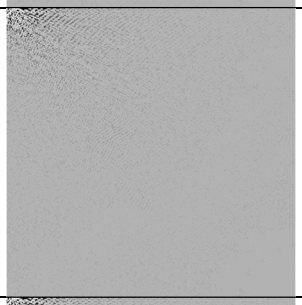
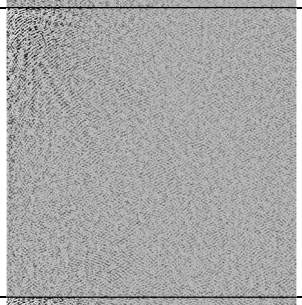
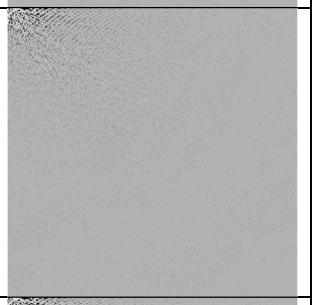
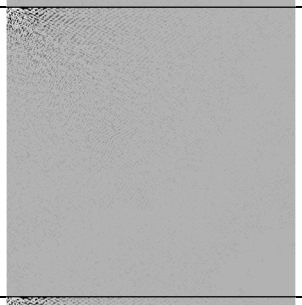
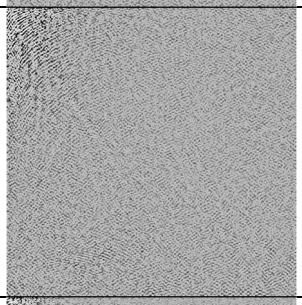
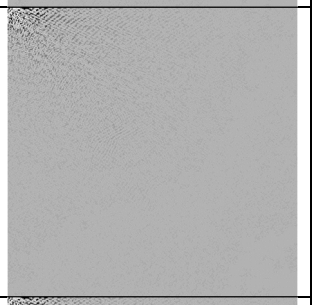
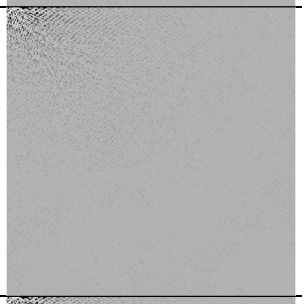
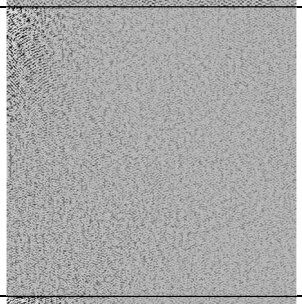
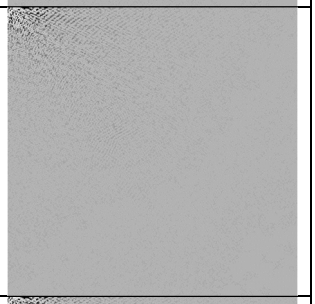
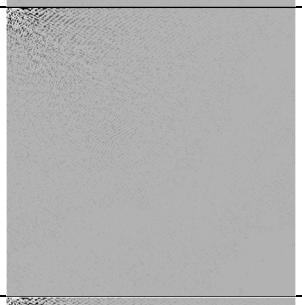
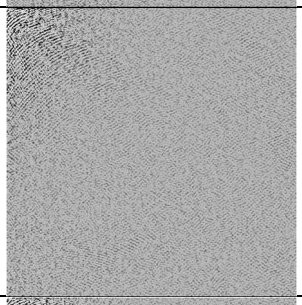
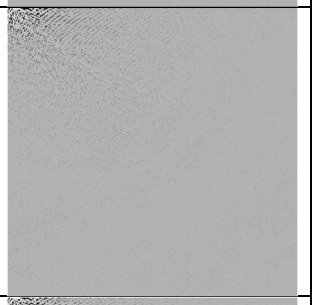
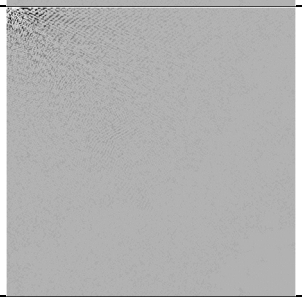
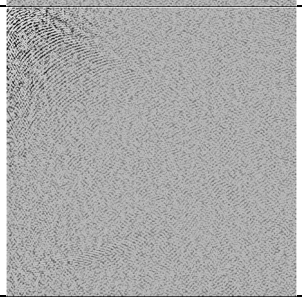
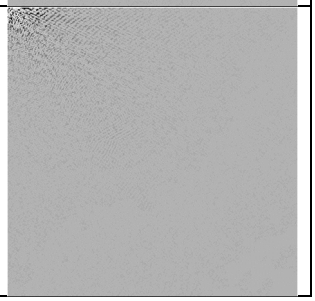
Setelah memperoleh *spectrum* magnitude dari masing-masing levelnya, tahap selanjutnya melakukan inverse *discrete cosine transform* yang bertujuan mengeembalikan *spectrum* magnitude menjadi domain spasial kembali. Tabel 3 menggambarkan perbandingan pada setiap levelnya citra *cover* sebelum dilakukan penyisipan data rahasia dan setelah dilakukan penyisipan. Jika diperhatikan secara seksama maka akan terlihat data rahasia sisipan pada citra *cover*. Semakin tinggi levelnya maka hasil penyisipannya tampak semakin jelas.

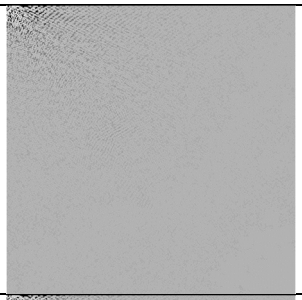
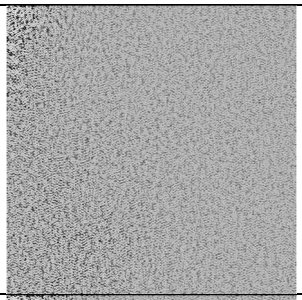
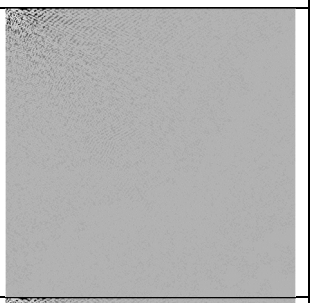
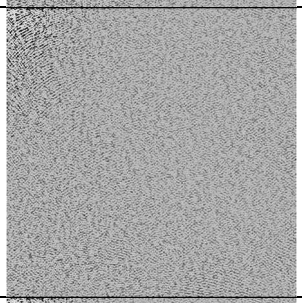
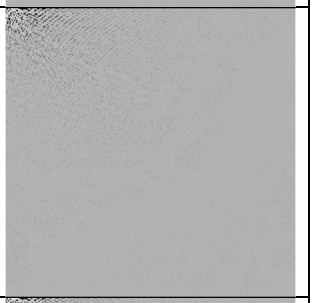
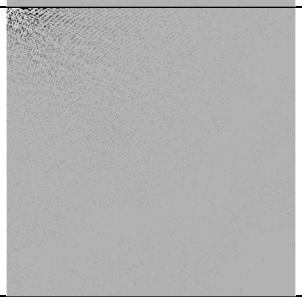
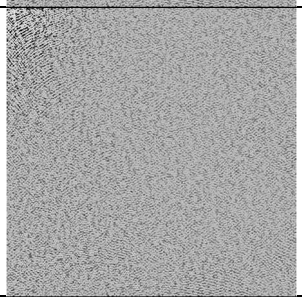
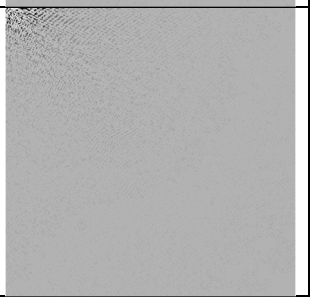
TABEL I
CITRA RAHASIA DOMAIN SPASIAL DAN SPEKTRUM MAGNITUDE

Level	Domain Spasial	Spektrum Magnitude	Level	Domain Spasial	Spektrum Magnitude
1			2		
3			4		
5			6		
7			8		
9					

TABEL II

SPEKTRUM MAGNITUDE SEBELUM, PENYISIPAN, DAN SETELAH PENYISIPAN

Level	Sebelum penyisipan	Penyisipan	Setelah penyisipan
1			
2			
3			
4			
5			
6			

Level	Sebelum penyisipan	Penyisipan	Setelah penyisipan
7			
8			
9			

Dalam melakukan pengujian analisis steganografi dengan metode *discrete* coosine *transform* dengan *multi-scale image* sharing ini, kami menggunakan tujuh parameter yaitu *Peak Signal to Noise Ratio*, *Mean Squared Error*, *Normalized Cross Correlation, Average Difference*, *Structural Content, Maximum Difference, Normalized Absolute Error*. Pengujian ini lakukan dengann menggunakan perangkat lunak Matlab untuk menganalisis hasil yang diperoleh.

A. Peak Signal to Noise Ratio (PSNR)

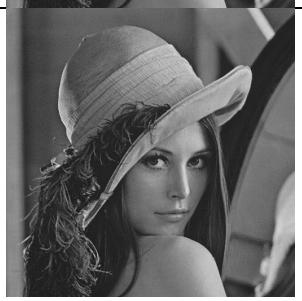
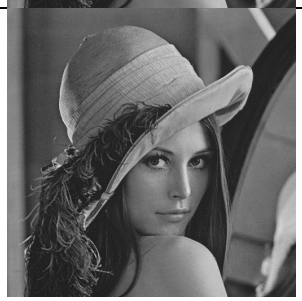
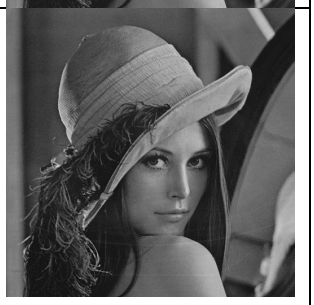
Peak Signal to Noise Ratio adalah perbansingan antara nilai maksimum sinyal yang diukur dengan besarnya derau yang berpengaruh pada sinyal tersebut[13],[14],[15],[16]. *Peak Signal to Noise Ratio* biasanya diukur dalam satuan *decibel*. *Peak Signal to Noise Ratio* juga sering digunakan dalam pengujian sistem kompresi dan rekontruksi. Pada penilitan ini *Peak Signal to Noise Ratio* digunakan untuk mengetahui kualitas citra dengan membandingkan citra sebelum mengalami proses *steganography* dan setelah proses *steganography*. *Peak Signal to Noise Ratio* memiliki persamaan seperti persamaan (3).

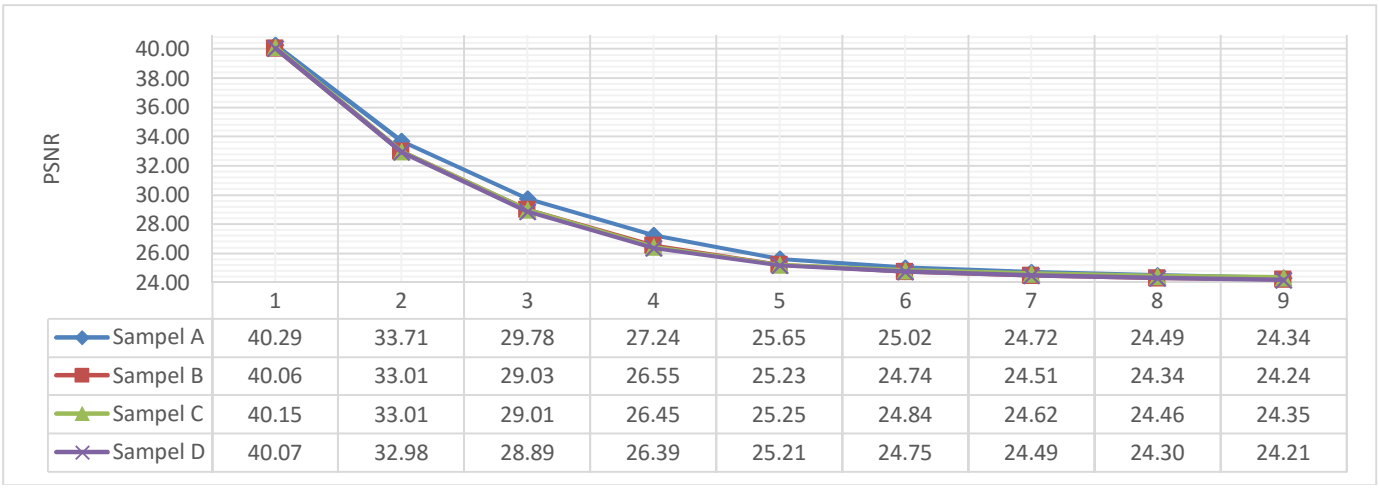
$$PSNR = 10 \log_{10} \frac{Max^2}{MSE} \quad (3)$$

Dimana Max adalah nilai maksimum piksel dari citra asli dan MSE adalah nilai dari *Mean Square Error*. Nilai dari MAX pada penelitian ini yaitu 512, karena citra yang digunakan memiliki ukuran 512px x 512px. Hasil dari PSNR dalam penelitian ini seperti pada grafik 1.

Dari grafik 1 menunjukan kualitas dari proses stehgenography setiap levelnya pada setiap masing-masing sampel. Proses *steganography* dengan *multi- level* diperoleh paling baik pada *level* 1 dengan nilai kurang lebih 40 db, sedangkan kualitas terburuk pada proses *steganography* pada *level* 9 dengan nilai kurang lebih 24 db. Semakin tinggi nilai PSNR maka kualitas steganpgraphy semakin baik, dan sebaliknya jika hasil steganogtahy emmiliki nilai PSNR yang rendah maka kualitas yang dihasilkan semakin buruk. Hasil grafik 1 memiliki tren grafik yang menurun sehingga dapat disimpulkan semakin banyak data (*multi- level*) yang disisipkan maka kualitas dari *steganography* semakin buruk.

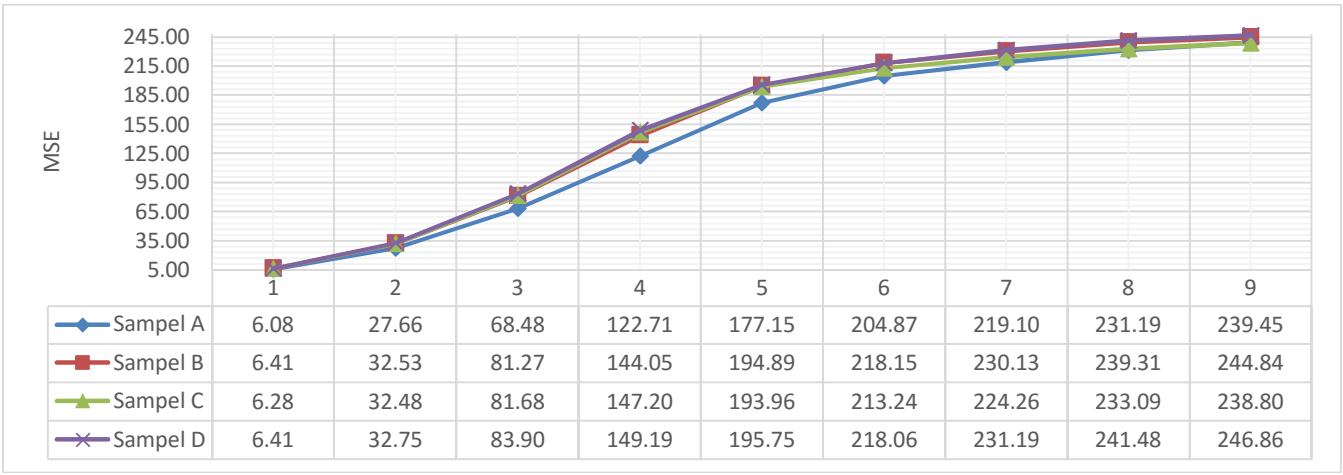
TABEL III
HASIL PENYISIPAN DOMAIN SPASIAL

Level	Sebelum penyisipan	Setelah penyisipan	Level	Sebelum penyisipan	Setelah penyisipan
1			2		
3			4		
5			6		
7			8		
9					



	1	2	3	4	5	6	7	8	9
Sampel A	40.29	33.71	29.78	27.24	25.65	25.02	24.72	24.49	24.34
Sampel B	40.06	33.01	29.03	26.55	25.23	24.74	24.51	24.34	24.24
Sampel C	40.15	33.01	29.01	26.45	25.25	24.84	24.62	24.46	24.35
Sampel D	40.07	32.98	28.89	26.39	25.21	24.75	24.49	24.30	24.21

Grafik 1. Hasil PSNR



	1	2	3	4	5	6	7	8	9
Sampel A	6.08	27.66	68.48	122.71	177.15	204.87	219.10	231.19	239.45
Sampel B	6.41	32.53	81.27	144.05	194.89	218.15	230.13	239.31	244.84
Sampel C	6.28	32.48	81.68	147.20	193.96	213.24	224.26	233.09	238.80
Sampel D	6.41	32.75	83.90	149.19	195.75	218.06	231.19	241.48	246.86

Garfik 2. Hasil MSE

B. Mean Squared Error (MSE)

Pada persamaan *Peak Signal to Noise Ratio* berkaitan dengan *Mean Square Error*. *Mean Square Error (MSE)* merupakan suatu metode pengukuran kontrol dan kualitas yang sudah dapat diterima luas[13],[11],[16]. *Mean Square Error dihitung* dihitung dari sebuah objek citra yang telah mengalami proses *steganography* selanjutnya dibandingkan dibandingkan dengan obek citra sebelum mengalami proses *steganography,* sehingga dapat diketahui tingkat ketidak sesuian antara kedua citra sebelum dan sesuah proses *steganography*. *Mean Square Error* memiliki persamaan (4).

$$MSE = \frac{1}{MN}\sum_{j=1}^{M}\sum_{k=1}^{N}\left(x_{j,k} - x'_{j,k}\right)^2 \quad (4)$$

Dimana M dan N adalah dimensi citra yang digunakan. $x_{j,k}$ adalah nilai piksel citra sebelum proses *steganography*. $x'_{j,k}$ adalah nilai piksel citra setelah mengalami proses *steganography.* Hasil dari MSE dalam penelitian ini seperti pada grafik 2.

MSE menurupakan salah satu evaluasi hasil *steganography* dimana proses ini menghitung error kuadrat rata-rata antara citra hasil dan citra sebelum steganpgraphy. Hasil MSE dari pengujian diperoleh penyisipan pada *level* 1 memiliki nilai kurang lebih 6 sedangkan nilai MSE dengan penyisipan pada *level* 9 memiliki nilai kurang lebih 240. Jika hasil MSE suatu citra *steganography* kecil maka citra *steganography* termasuk baik dan jika hasil MSE citra *steganography* semakin besar maka error citra yang dihasilkan semakin besar pulan dan termasuk tidak baik (buruk). Hasil dari Grafik 2 menunujukan tren nilai MSE yang meningkat pada setiap levelnya sehingga dapat disimpulkan semakin banyak proses penyisipan *multi-level*nya maka error yang dihasilkan semakin besar.

C. Normalized Cross Correlation (NCC)

Normalized Cross Correlation[16] memiliki persamaan seperti persamaan (5).

$$NCC = \sum_{j=1}^{M}\sum_{k=1}^{N}\left(x_{j,k} - x'_{j,k}\right)\frac{1}{\sum_{j=1}^{M}\sum_{k=1}^{N}\left(x_{j,k}\right)} \quad (5)$$

Dimana M dan N adalah dimensi citra yang digunakan. $x_{j,k}$ adalah nilai piksel citra sebelum proses *steganography*. $x'_{j,k}$ adalah nilai piksel citra setelah mengalami proses *steganography*. Hasil dari NCC dalam penelitian ini seperti pada grafik 3.

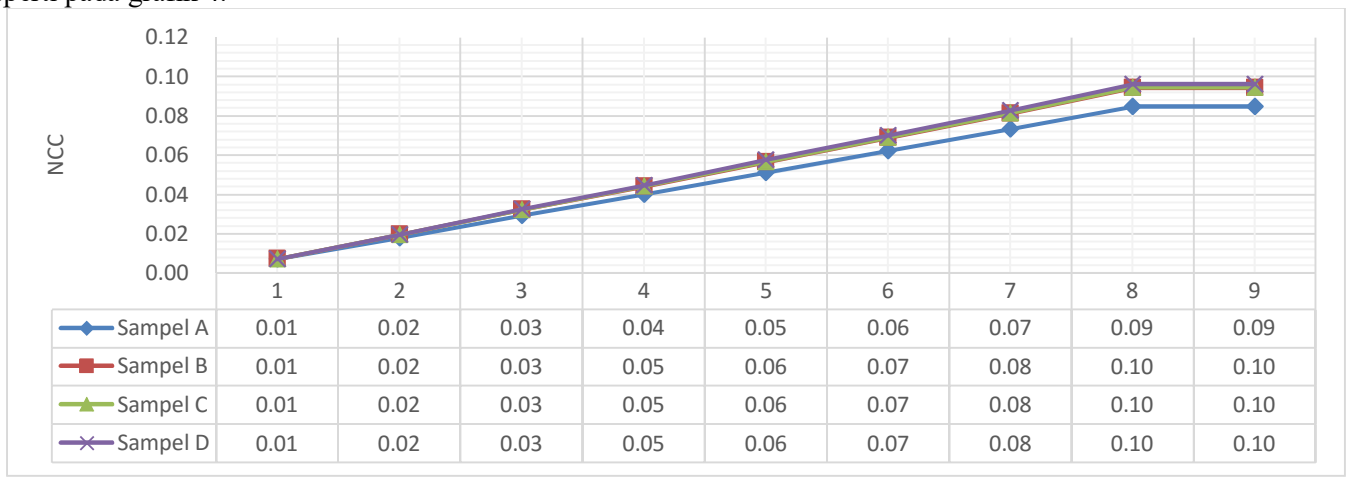
NCC merupakan salah satu evaluasi hasil *steganography* dimana proses ini menghitung korelasi kesamaan antara 2 buah citra yaitu citra asli dan citra hasil steganpography. Hasil NCC dari pengujian diperoleh penyisipan pada level 1 memiliki nilai kurang lebih 0.01 sedangkan nilai NCC dengan penyisipan pada level 8 dan 9 memiliki nilai kurang lebih 0.1. Jika hasil NCC suatu citra *steganography* kecil maka citra *steganography* termasuk baik dan jika hasil NCC citra *steganography* semakin besar maka korelasi antara citra yang dihasilkan semakin jauh (buruk). Hasil dari Grafik 3 menunujukan tren nilai NCC yang meningkat pada setiap levelnya sehingga dapat disimpulkan semakin banyak proses penyisipan *multi-level*nya maka korelasi antara citra asli dan citra *steganography* yang dihasilkan semakin jauh.

D. *Average Difference (AD)*

Average Difference[16] memiliki persamaan seperti persamaan (6).

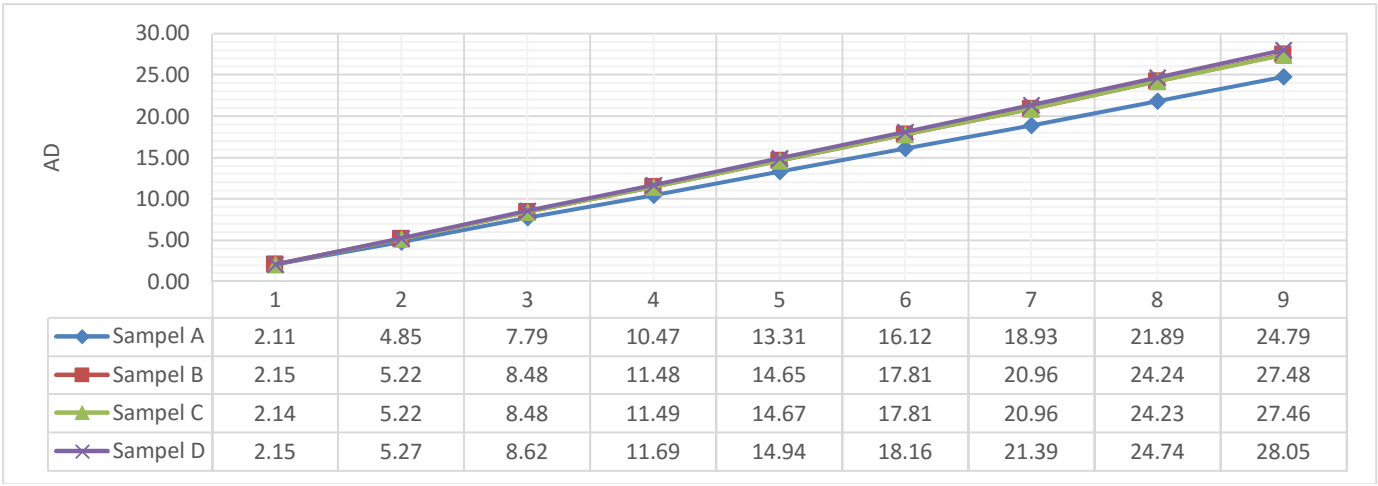
$$AD = \sum_{j=1}^{M}\sum_{k=1}^{N}\left(x_{j,k} - x'_{j,k}\right)/MN \quad (6)$$

Dimana M dan N adalah dimensi citra yang digunakan. $x_{j,k}$ adalah nilai piksel citra sebelum proses *steganography*. $x'_{j,k}$ adalah nilai piksel citra setelah mengalami proses *steganography*. Hasil dari AD dalam penelitian ini seperti pada grafik 4.



	1	2	3	4	5	6	7	8	9
Sampel A	0.01	0.02	0.03	0.04	0.05	0.06	0.07	0.09	0.09
Sampel B	0.01	0.02	0.03	0.05	0.06	0.07	0.08	0.10	0.10
Sampel C	0.01	0.02	0.03	0.05	0.06	0.07	0.08	0.10	0.10
Sampel D	0.01	0.02	0.03	0.05	0.06	0.07	0.08	0.10	0.10

Grafik 3. Hasil NCC



	1	2	3	4	5	6	7	8	9
Sampel A	2.11	4.85	7.79	10.47	13.31	16.12	18.93	21.89	24.79
Sampel B	2.15	5.22	8.48	11.48	14.65	17.81	20.96	24.24	27.48
Sampel C	2.14	5.22	8.48	11.49	14.67	17.81	20.96	24.23	27.46
Sampel D	2.15	5.27	8.62	11.69	14.94	18.16	21.39	24.74	28.05

Grafik 4. Hasil AD

AD menurupakan salah satu evaluasi hasil *steganography* dimana proses ini menghitung rata-rata selisih intensitas antara 2 buah citra yaitu citra asli dan citra hasil steganpography. Hasil AD dari pengujian diperoleh penyisipan pada level 1 memiliki nilai kurang lebih 2.15 sedangkan nilai AD dengan penyisipan pada *level* 9 memiliki

nilai kurang lebih 27.47. Jika hasil AD suatu citra *steganography* kecil maka citra *steganography* memiliki rata-rata intensitas antara dua citra kecil(baik) dan jika hasil AD citra *steganography* semakin besar maka nilai rata-rata selisih intensitas antara citra yang dihasilkan semakin tinggi (buruk). Hasil dari Grafik 4 menunujukan tren nilai AD yang meningkat pada setiap *level*nya sehingga dapat disimpulkan semakin banyak proses penyisipan *multi-level*nya maka nilai rata-rata selisih antara citra asli dan citra *steganography* yang dihasilkan semakin tinggi.

E. Structural Content (SC)

Structural Content[16] memiliki persamaan seperti persamaan (7).

$$SC = \sum_{j=1}^{M}\sum_{k=1}^{N}(x_{j,k} - x'_{j,k}) / \sum_{j=1}^{M}\sum_{k=1}^{N}(x'_{j,k})^2 \quad (7)$$

Dimana M dan N adalah dimensi citra yang digunakan. $x_{j,k}$ adalah nilai piksel citra sebelum proses *steganography*. $x'_{j,k}$ adalah nilai piksel citra setelah mengalami proses *steganography*. Hasil dari SC dalam penelitian ini seperti pada grafik 5.

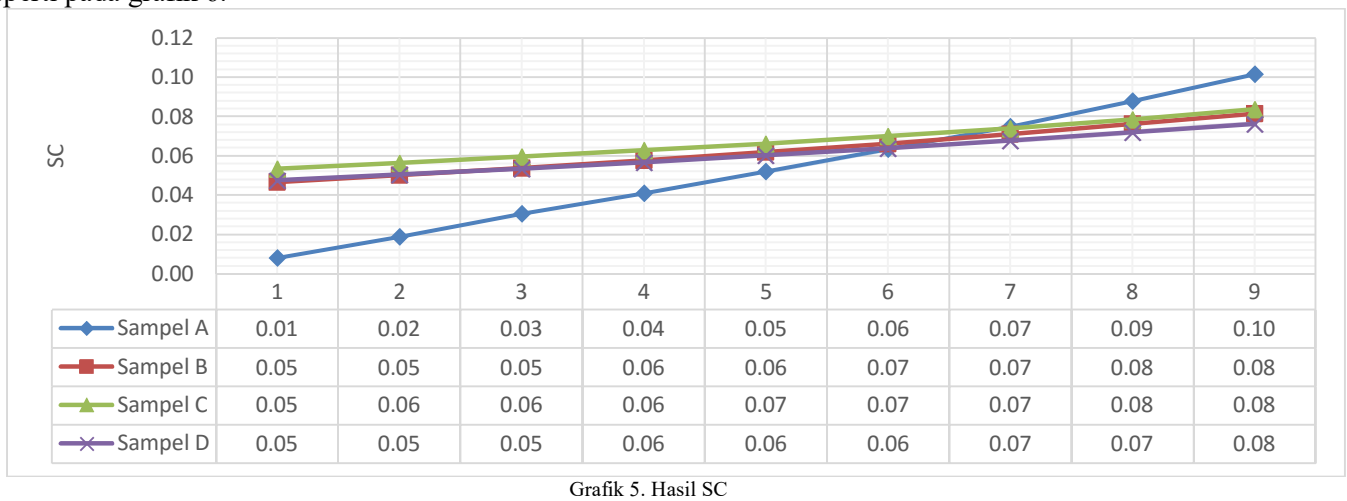
SC menurupakan salah satu evaluasi hasil *steganography* dimana proses ini menghitung rasio dari struktul konten informasi antara 2 buah citra yaitu citra asli dan citra hasil steganpography. Hasil SC dari pengujian diperoleh penyisipan pada *level* 1 memiliki nilai kurang lebih 0.05 sedangkan nilai SC dengan penyisipan pada *level* 9 memiliki nilai kurang lebih 0.08. Jika hasil SC suatu citra *steganography* kecil maka citra *steganography* memiliki rasio dari struktul konten informasi antara dua citra kecil (baik) dan jika hasil SC citra *steganography* semakin besar maka nilai rasio dari struktul konten informasi antara citra yang dihasilkan semakin tinggi (buruk). Hasil dari Grafik 5 menunujukan tren nilai SC yang meningkat pada setiap *level*nya sehingga dapat disimpulkan semakin banyak proses penyisipan *multi-level*nya maka nilai rasio dari struktul konten informasi antara citra asli dan citra *steganography* yang dihasilkan semakin buruk.

F. Maximum Difference (MD)

Structural Content[16] memiliki persamaan seperti persamaan (8).

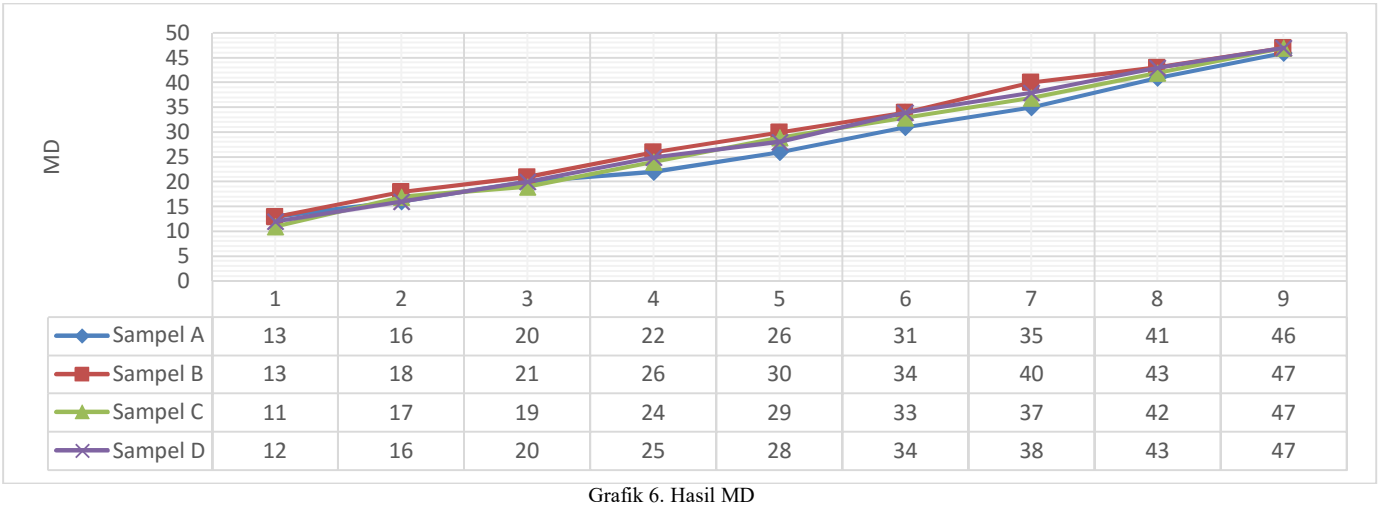
$$MD = MAX(|x_{j,k} - x'_{j,k}|) \quad (8)$$

Dimana M dan N adalah dimensi citra yang digunakan. $x_{j,k}$ adalah nilai piksel citra sebelum proses *steganography*. $x'_{j,k}$ adalah nilai piksel citra setelah mengalami proses *steganography*. Hasil dari MD dalam penelitian ini seperti pada grafik 6.



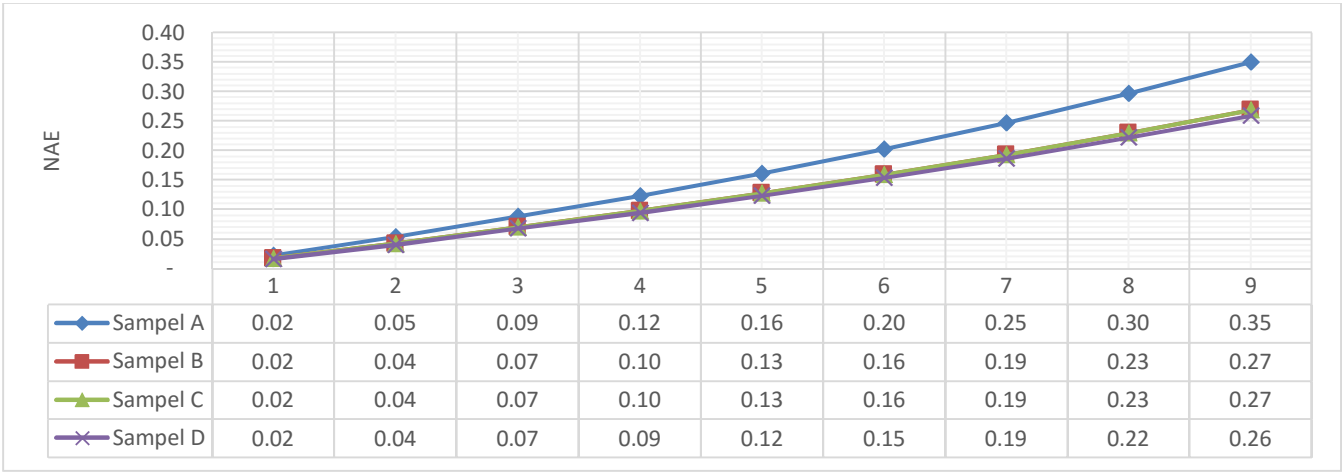
	1	2	3	4	5	6	7	8	9
Sampel A	0.01	0.02	0.03	0.04	0.05	0.06	0.07	0.09	0.10
Sampel B	0.05	0.05	0.05	0.06	0.06	0.07	0.07	0.08	0.08
Sampel C	0.05	0.06	0.06	0.06	0.07	0.07	0.07	0.08	0.08
Sampel D	0.05	0.05	0.05	0.06	0.06	0.06	0.07	0.07	0.08

Grafik 5. Hasil SC



	1	2	3	4	5	6	7	8	9
Sampel A	13	16	20	22	26	31	35	41	46
Sampel B	13	18	21	26	30	34	40	43	47
Sampel C	11	17	19	24	29	33	37	42	47
Sampel D	12	16	20	25	28	34	38	43	47

Grafik 6. Hasil MD



	1	2	3	4	5	6	7	8	9
Sampel A	0.02	0.05	0.09	0.12	0.16	0.20	0.25	0.30	0.35
Sampel B	0.02	0.04	0.07	0.10	0.13	0.16	0.19	0.23	0.27
Sampel C	0.02	0.04	0.07	0.10	0.13	0.16	0.19	0.23	0.27
Sampel D	0.02	0.04	0.07	0.09	0.12	0.15	0.19	0.22	0.26

Grafik 7. Hasil NAE

MD menurupakan salah satu evaluasi hasil *steganography* dimana proses ini menghitung jarak selisih korelasi antara 2 buah citra yaitu citra asli dan citra hasil steganpography. Hasil MD dari pengujian diperoleh penyisipan pada *level* 1 memiliki nilai kurang lebih 13 sedangkan nilai MD dengan penyisipan pada *level* 9 memiliki nilai kurang lebih 47. Jika hasil MD suatu citra *steganography* kecil maka citra *steganography* termasuk baik dan jika hasil MD citra *steganography* semakin besar maka jarak selisih korelasi antara citra yang dihasilkan semakin jauh (buruk). Hasil dari Grafik 6 menunujukan tren nilai MD yang meningkat pada setiap levelnya sehingga dapat disimpulkan semakin banyak proses penyisipan *multi-level* nya maka jarak selisih korelasi antara citra asli dan citra *steganography* yang dihasilkan semakin jauh.

G. *Normalized Absolute Error (NAE)*

Nomalized Absolute Error[16] memiliki persamaan seperti persamaan (9).

$$NAE = \sum_{j=1}^{M}\sum_{k=1}^{N}|x_{j,k} - x'_{j,k}| / \sum_{j=1}^{M}\sum_{k=1}^{N}|x'_{j,k}| \quad (9)$$

Dimana M dan N adalah dimensi citra yang digunakan. $x_{j,k}$ adalah nilai piksel citra sebelum proses *steganography*. $x'_{j,k}$ adalah nilai piksel citra setelah mengalami proses *steganography*. Hasil dari MD dalam penelitian ini seperti pada grafik 7.

NAE menurupakan salah satu evaluasi hasil *steganography* dimana proses ini menghitung kualitas antara 2 buah citra yaitu citra asli dan citra hasil steganpography. Hasil NAE dari pengujian diperoleh penyisipan pada *level* 1 memiliki nilai kurang lebih 0.02 sedangkan nilai NAE dengan penyisipan pada *level* 9 memiliki nilai kurang lebih 0.27. Jika hasil NAE suatu citra *steganography* kecil maka citra *steganography* memiliki kualitas antara dua citra kecil (baik) dan jika hasil NAE citra *steganography* semakin besar maka nilai kualitas antara citra yang dihasilkan semakin tinggi (buruk). Hasil dari Grafik 7 menunujukan tren nilai NAE yang meningkat pada setiap levelnya sehingga dapat disimpulkan semakin banyak proses penyisipan *multi-level*nya maka nilai kualitas antara citra asli dan citra *steganography* yang dihasilkan semakin buruk.

TABEL IV
HASIL SIZE PADA SETIAP *LEVEL*

Level	Size sampel A (*bytes*)		Size sampel B (*bytes*)		Size sampel C (*bytes*)		Size sampel D (*bytes*)	
	Sebelum	Sesudah	Sebelum	Sesudah	Sebelum	Sesudah	Sebelum	Sesudah
1	95,388	95,774	154,954	155,147	111,758	112,270	110,938	111,189
2	95,388	95,672	154,954	154,641	111,758	111,850	110,938	110,923
3	95,388	95,632	154,954	154,097	111,758	111,762	110,938	110,665
4	95,388	95,677	154,954	153,658	111,758	111,642	110,938	110,380
5	95,388	95,679	154,954	153,154	111,758	111,211	110,938	110,142
6	95,388	95,538	154,954	152,607	111,758	111,012	110,938	109,700
7	95,388	95,808	154,954	152,231	111,758	110,911	110,938	109,483
8	95,388	96,044	154,954	151,783	111,758	110,815	110,938	109,340
9	95,388	96,169	154,954	151,268	111,758	110,666	110,938	109,033

H. Size

Salah satu parameter dalam pengujian hasil ialah ukuran dari citra. Pada grafik 8 menunjukan hasil ukuran yang digunakan dengan berbagai format.

Tabel 4 diatas menunjukan hasil ukuran dari citra *multi-level steganography* pada 4 buah sampel citra. Hasil tersebut menunjukan terjadi perubahan ukuran pada setiap levelnya, semakin banyak penyembuanyian data pada masing-masing levelnya maka ukuran *file* citra *steganography* semakin besar pula.

V. KESIMPULAN DAN SARAN

Metode yang ditawarkan ini telah memberikan hasil yang cukup baik dalam melakukan penyisipan *file* citra medis rahasia yang berjumalah lebih dari satu dengan skema *multi-scale image* sharing (MSIS). Pengunaan *discrete cosine transform* dalam domain frekuensi dirasa efektif pada proses penyisipan *file* medis rahasia. Dalam hal kualitas maupun dalam hal ukuran *file* citra hasil *steganography* metode yang ditawarkan ini memberikan hasil yang baik. Hal ini ditunjukan dengan hasil PNSR pada penyisipan *level* 1 dan *level* 9 bernilai kurang lebih 40 db dan 24 db, hasil MSE pada penyisipan *level* 1 dan *level* 9 bernilai kurang lebih 6.41 dan 240, hasil NCC pada penyisipan *level* 1 dan *level* 9 bernilai kurang lebih 0.01 dan 0.1, hasil AD pada penyisipan *level* 1 dan *level* 9 bernilai kurang lebih 2.15 dan 27.46, hasil SC pada penyisipan *level* 1 dan *level* 9 bernilai kurang lebih 0.05 dan 0.08, hasil MD pada penyisipan *level* 1 dan *level* 9 bernilai kurang lebih 13 db dan 47, hasil NAE pada penyisipan *level* 1 dan *level* 9 bernilai kurang lebih 0.02 dan 0.27. Saran untuk penelitian selanjutnya adalah mengembangkan metode ini dengan domain frekuensi lainnya, seperti *discrete wavelet transform*, atau *discrete wavelet transform*.

DAFTAR PUSTAKA

[1] G. Huayong, "Steganography and Steganalysis based on digital *image*," *Image Signal …*, pp. 252–255, 2011.

[2] C.-H. Zeng, Yi-Chong ; Tsai, "High Capacity *Multi-Scale Image* Sharing Scheme by Combining Visual Cryptography with Data Hiding," pp. 4536–4539, 2013.

[3] A. I. Iliev, M. S. Scordilis, dan C. Gables, "*Multi Level* High Capacity Data Hiding Technique for Stereo Audio," pp. 1793–1797, 2004.

[4] C. Chen, "*Multi*-morphological *Image* Data Hiding based on the Application of Rubik ' s Cubic Algorithm," no. 1, pp. 135–139, 2012.

[5] K. Jung, K. Ha, dan K. Yoo, "*Image* Data Hiding Method Based on *Multi-pixel* Differencing and LSB," pp. 355–358, 2008.

[6] X. Zeng, Z. Li, dan L. Ping, "Reversible data hiding scheme using reference *pixel* and *multi*-layer embedding," *AEUE - Int. J. Electron. Commun.*, vol. 66, no. 7, pp. 532–539, 2012.

[7] C. Lin, W. Tai, dan C. Chang, "*Multi-level* reversible data hiding based on histogram modification of difference *image*s," vol. 41, pp. 3582–3591, 2008.

[8] C. Lee, Chin-feng;Chang, Chin-Chen ;Gao, "A Two-staged *Multi-level* Reversible Data Hiding Exploiting Lagrange Interpolation," pp. 6–9, 2013.

[9] M. A. Alavianmehr dan M. Rezaei, "A Semi-Fragile Lossless Data Hiding Scheme Based on *Multi-level* Histogram Shift in *Image* Integer *Wavelet Transform* Domain," pp. 976–981, 2012.

[10] L. Rura, B. Issac, dan M. Haldar, "Analysis of *image* steganography techniques in secure online voting," *Comput. Sci. Netw. …*, 2011.

[11] A. a. J. Altaay, S. Bin Sahib, dan M. Zamani, "An Introduction to *Image* Steganography Techniques," *2012 Int. Conf. Adv. Comput. Sci. Appl. Technol.*, pp. 122–126, Nov. 2012.

[12] A. B. Watson, "*Image* Compression Using the Discrete *Cosine Transform*," vol. 4, no. 1, pp. 81–88, 1994.

[13] S. Kumar dan S. K. Muttoo, "Data Hiding Techniques Based on *Wavelet*-like *Transform* and Complex *Wavelet Transform*s," *2010 Int. Symp. Intell. Inf. Process. Trust. Comput.*, pp. 1–4, Okt. 2010.

[14] H. Noda dan T. Furuta, "Application of BPCS steganography to *wavelet* compressed video," *Image Process. 2004. …*, no. 1, pp. 1–4, 2004.

[15] P. Shi, Z. Li, dan T. Zhang, "A technique of improved steganography text based on chaos and BPCS," *Adv. Comput. Control (ICACC), …*, pp. 232–236, 2010.

[16] A. Nagar, "A Modified Secure Digital *Image* Steganography Based on Discrete *Wavelet Transform*," pp. 1096–1100, 2012.